Paul B. Barton, OSB No. 100502
Alex Graven, OSB No. 153443
OLSEN BARTON LLC
4035 Douglas Way, Suite 200
Lake Oswego, OR 97035
Tel: (503) 468-5573
Fax: (503) 820-2933
paul@olsenbarton.com
alex@olsenbarton.com

Mason A. Barney *(pro hac vice to be filed)*
Tyler J. Bean *(pro hac vice to be filed)*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Attorneys for Plaintiff, individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

DEBORAH CIMINO, individually, and on behalf of all others similarly situated, Plaintiff, v. ETZ HAYIM HOLDINGS, S.P.C., d/b/a LAZARUS NATURALS Defendant.	**Case No:** **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Deborah Cimino brings this Class Action Complaint against ETZ Hayim Holdings, S.P.C., d/b/a Lazarus Naturals ("Defendant" or "Lazarus Naturals"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This is a class action for damages with respect to Defendant and its failure to exercise reasonable care in securing sensitive personal information including without limitation, unencrypted and unredacted name, billing and shipping address, and financial information such as credit or debit card information (including card number, expiration date and printed card security code) (collectively, "personal identifiable information" or "PII").

2. Plaintiff seeks damages for herself and other similarly situated individuals impacted in the data breach at issue (referred to herein as the "Class Members," "Class," or "Classes"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive personal identifiable information of Plaintiff and the Class.

3. On or about August 3, 2023, Lazarus Naturals sent notice letters to Plaintiff and Class Members regarding widespread and unauthorized "access or acquisition" of its website (the "Data Breach") involving Plaintiff's and Class Members' sensitive PII ("Notice"). The number of individuals affected by the Data Breach is estimated to be 42,000.[1]

///

[1] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/3e1fc8e0-4548-4f71-b116-8ff2802ba6d8.shtml (last visited (last visited August 14, 2023).

4. Lazarus Naturals explains in the Notice that on July 10, 2023, it discovered that "one or more malicious actors" exploited a software vulnerability on its website, allowing the threat actors to facilitate the compromise of Plaintiff's and Class Members' PII. This unauthorized access and acquisition took place between March 1 and June 2, 2023.

5. Plaintiff and Class Members are current and former Lazarus Naturals users who purchased products from Lazarus Naturals through its website.

6. In this era of frequent data security attacks and data breaches, including a similar data breach that impacted Lazarus Naturals only a few years earlier,[2] Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

7. Upon information and belief, Plaintiff's and Class Members' PII that was compromised in the Data Breach was unencrypted and unredacted and was acquired by the threat actors due to Lazarus Naturals' negligent and/or careless acts and omissions.

8. Upon information and belief, based on the type of sophisticated and malicious criminal activity apparent here, the type of PII targeted, Defendant's admission that the PII was accessed, and reports of criminal misuse of Plaintiff's and Class Members' data following the Data Breach, it can be concluded that Plaintiff's and Class Members' PII was accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

9. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, disseminated on the dark web, and subsequently misused. Indeed, Class Members have suffered actual identity theft and misuse of their data following the Data Breach.

[2] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/246c9db7-a087-4f19-a9d4-657873ccb522.shtml (last visited (last visited August 14, 2023).

10. As a result of the Data Breach and in light of the fraud and identity theft already experienced by Plaintiff Cimino, which is explained in greater detail *infra*, Plaintiff and the Class Members are also at an imminent risk of future identity theft.

11. As Defendant instructed, advised, and warned in its Notice,[3] Plaintiff and the Class Members must now closely monitor their financial accounts to guard against additional identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include in the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding and mitigating against the imminent risk of identity theft.

12. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time heeding Defendant's warnings and following its instructions in the Notice letter; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches similar to this Data Breach and Lazarus Naturals' 2020 data breach, so long as Defendant continues to fail to undertake appropriate and adequate measures to protect its customers' PII.

[5] *Notice of Data Event*, Lazarus Naturals Ticketing Corporation, https://apps.web.maine.gov/online/aeviewer/ME/40/3034e32e-3694-4dd1-82f6-9a1c756dced4/1dbbc7c8-25a0-4d38-bb49-1a1a0ddd5b5a/document.html (last visited August 9, 2023).

13. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of herself and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief, including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

PARTIES

14. Plaintiff Deborah Cimino is a citizen of Florida. Ms. Newman received Lazarus Naturals' Notice of Data Security Incident on or about August 5, 2023 by mail.

15. Defendant Lazarus Naturals is an Oregon-based supplier of CBD products, with its principal place of business at 16427 NE Airport Way, Portland, OR 97230.

16. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332, the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Class Member and Defendant are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1367.

18. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because Defendant resides in this District.

19. Defendant is subject to personal jurisdiction in Oregon because defendant is incorporated and/or is domiciled in this state and conducts substantial business in Oregon and within this District through its offices, subsidiaries and affiliates.

FACTUAL ALLEGATIONS

Defendant's Promises

20. Defendant operates its business nationwide, offering an online website where products can be purchased.

21. Plaintiff and the Class Members, as current or former Lazarus Naturals users, reasonably relied (directly or indirectly) on Defendant to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Users like Plaintiff, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

22. Indeed, Lazarus Naturals promotes to its users that it takes the privacy and security of PII seriously, stating its platform is secure and PCI-DSS compliant.[4]

23. Defendant's Privacy Policy ("Privacy Policy") also states that it will take "reasonable precautions and follow industry best practices to make sure [customer information] is not inappropriately lost, misused, accessed, disclosed, altered or destroyed."[5]

The Data Breach

24. On or about August 3, 2023, Defendant notified Plaintiff and Class Members about a widespread data breach of its website involving the sensitive personally identifiable information of its customers.

[4] Lazarus Naturals, *Privacy Policy*, https://www.lazarusnaturals.com/policies#privacy (last visited August 14, 2023)
[5] *Id*.

25. The Data Breach occurred between "March 1, 2023 and June 2, 2023" through the exploitation of a software vulnerability on Defendant's website, which allowed the "malicious actors" to insert malicious code facilitating the compromise.

26. The Notice Defendant directed to be sent to Lazarus Naturals users, including Plaintiff and Class Members, noted that their PII was "accessed or acquired" by way of the Data Breach. Thus, Defendant violated its own Privacy Policy.

27. Plaintiff and Class Members in this action were, upon information and belief, current and former Lazarus Naturals users whose PII was utilized by Lazarus Naturals for purposes of providing services. Plaintiff and Class Members first learned of the Data Breach when they received the Notice on or about August 5, 2023.

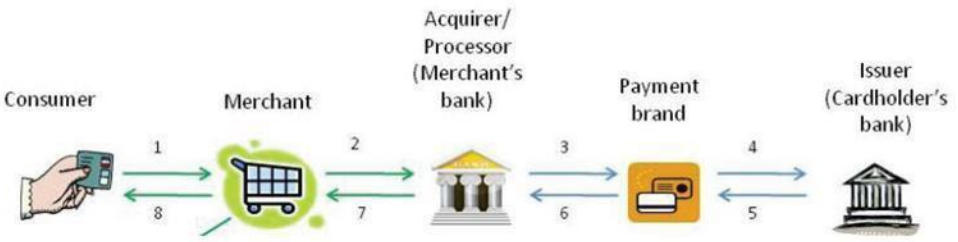
28. Upon information and belief, the PII was not encrypted prior to the Data Breach. Lazarus Naturals did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

29. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and Class Members.

Securing PII and Preventing Breaches

30. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped," and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (i.e., the retailer's bank). The acquirer relays the

transaction information to the payment card company, who then sends the information to the issuer (i.e., cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. See graphic below:[6]



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

31. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer, and it is placed into some form of storage in the merchant's servers.

32. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment

[6] Payments 101: Credit and Debit Card Payments, First Data, at 7 (Oct. 2010), http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf (last visited August 9, 2023).

it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers. Defendant failed to implement such a simple solution, which would have protected its customers' data.

33. The financial fraud already suffered by Plaintiff and other Lazarus Naturals customers demonstrates that Defendant chose not to invest in the technology to encrypt payment card data at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of payment card data; and/or failed to learn from the mistakes it made leading to the 2020 data breach.

34. These failures also demonstrate, despite what Defendant's Privacy Policy states, a clear violation of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles payment card data.

///

///

///

///

///

///

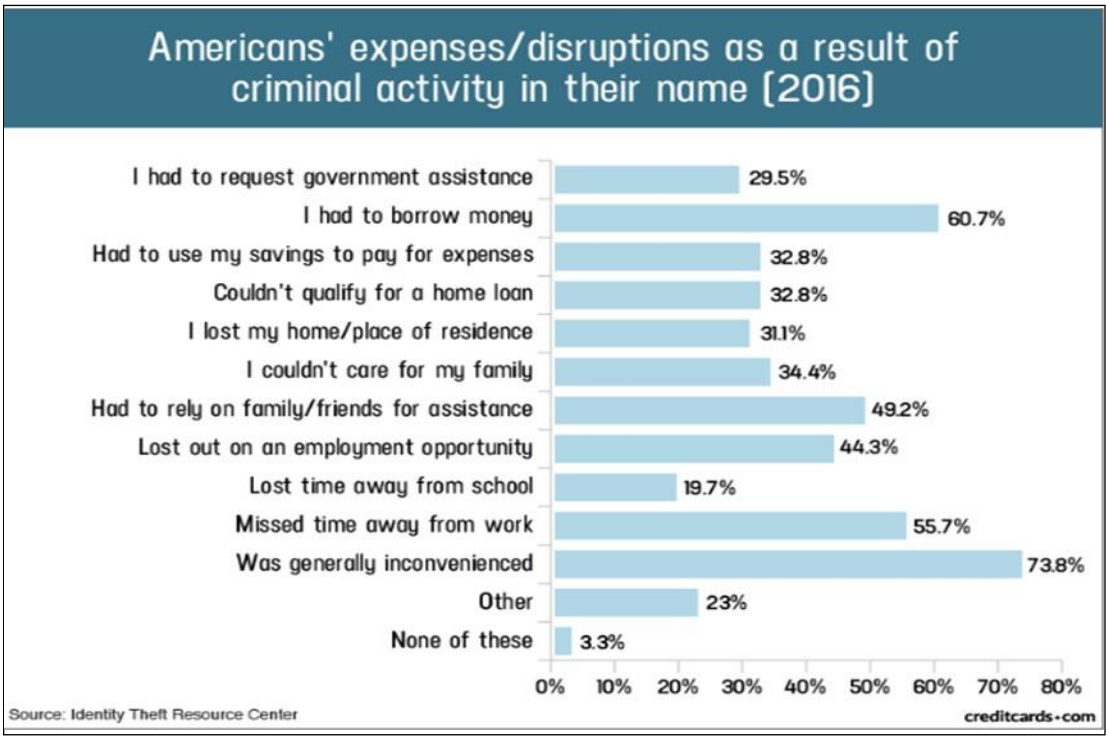
///

///

///

Plaintiff's and Class Members' Harms

35. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII:[7]



36. Plaintiff and Class Members have experienced one or more of these harms as a result of the Data Breach.

37. Furthermore, theft of PII is also gravely serious. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

[7] Jason Steele, *Credit Card Fraud and ID Theft Statistics*, CREDITCARDS.COM (June 11, 2021), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ [https://web.archive.org/web/20200918073034/https://www.creditcards.com/credit-card-news/credit-card- security-id-theft-fraud-statistics-1276/].

38. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

39. PII is a such valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

40. There is a strong probability that entire batches of stolen payment card information, full names, email addresses, and billing and shipping addresses have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and/or sophisticated targeting phishing schemes for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial and other accounts for many years to come at a level that was not necessary before the Data Breach.

41. Plaintiff and Class Members have suffered and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims have and will continue to spend substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

[8] U.S. Gov't Accountability Off., GAO 07737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

42. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

43. Plaintiff's and Class Members' PII was compromised as a direct and proximate result of the Data Breach.

44. As a direct and proximate result of the Data Breach, Plaintiff's PII was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiff and Class Members.

45. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiff and Class Members now have to take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying

financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

46. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

47. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

48. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff and Defendant included Defendant's contractual obligation to provide adequate data security in exchange for Plaintiff's and Class Members' payments submitted via Defendant's website, which data security Defendant failed to provide. Thus, Plaintiff and the Class Members did not get what they paid for.

49. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

50. Plaintiff and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property, including PII;

b. Improper disclosure of their PII property;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' PII being placed in the hands of criminals;

d. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' PII for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

51. The substantial delay in providing notice of the Data Breach deprived Plaintiff and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

52. It is well known that PII, including name, contact, and payment information in particular, is an invaluable commodity and a frequent target of hackers.

53. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June

2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), as well as its own recent data breach in 2020, Defendant knew or should have known that its systems would be targeted by cybercriminals.

54. Indeed, cyberattacks against the retail industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime."[9]

55. Moreover, it is well-known that the specific PII at issue in this case, including names, contact, and payment information in particular, is a valuable commodity and a frequent target of hackers.

56. As an online platform that collects, utilizes, and stores particularly sensitive PII, Defendant was at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect the PII of Plaintiff and Class Members.

57. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

///

///

[9] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit, FBI* (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

The Value of Personal Identifiable Information

58. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

59. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.

60. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

61. A dishonest person who has your name and contact information can use it to get other personal information about you. A breach including this type of information places data breach victims at an increased risk of phishing and social engineering attacks, eventually leading to identity theft. Moreover, the PII affected by this Data Breach included payment information, which no doubt leads to thousands of dollars in unauthorized transactions which victims are left to spend time disputing or paying for.

///

///

Defendant Failed to Comply with Recognized Security Standards

62. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

63. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

64. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs;

j. Monitoring for server requests from TOR exit nodes; and

k. Monitoring and auditing the programming of its website(s).

65. Upon information and belief, Defendant failed to comply with one or more of these standards.

Lazarus Naturals Failed to Comply with FTC Guidelines

66. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

67. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

68. The FTC has brought well-publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

69. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses. There, the FTC

[10] 17 C.F.R. § 248.201 (2013).
[11] *Id.*

advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software; and

(n) Implementing multi-factor authentication.

70. Upon information and belief, Defendant failed to implement or adequately implement at least one of these fundamental data security practices.

71. Defendant's failure constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

72. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent. In fact, Plaintiff and Class Members have already been victims of identity theft in the form of unauthorized transactions on the same debit or credit cards used on Defendant's platform.

73. Given the type of targeted attack in this case, the sophisticated criminal activity, and the type of PII at issue, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to continue to fraudulently misuse the PII to target Plaintiff and Class Members with sophisticated phishing and social engineering attacks.

74. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names, combined with contact information like billing and shipping addresses and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts and target them in elaborate phishing social engineering schemes.

75. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

76. To date, Defendant has done very little to adequately protect Plaintiff and Class Members or to compensate them for their injuries sustained in this Data Breach.

77. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

78. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

79. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

80. Plaintiff's mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

81. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its products and services, Plaintiff and other reasonable consumers understood and expected that they were also paying for the security of the PII they were entrusting to Defendant when, in fact, Defendant did not provide

nor invest in the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than that for which they reasonably bargained.

82. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiff and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant once again fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

Plaintiff Deborah Cimino's Experience

83. Plaintiff Cimino provided her PII to Lazarus Naturals in conjunction with the products she purchased from Defendant's website.

84. As part of her involvement with Defendant as a consumer, Plaintiff entrusted her PII, and other confidential information such as name, billing and shipping address, e-mail address, and payment card information, to Defendant with the reasonable expectation and understanding that Defendant would at least take industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure and timely notify her of any data security incidents related thereto.

85. Plaintiff would not have entrusted her PII to Lazarus Naturals had she known Lazarus Naturals would not take reasonable steps to safeguard her PII.

86. On or about August 5, 2023, roughly *five months* after Defendant's Data Breach began, Plaintiff Cimino received a Notice from Defendant notifying her that her PII had been improperly accessed and taken by third parties.

87. As a result of the Data Breach, Plaintiff Cimino has been forced to take reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, changing passwords to all of her accounts, and reviewing financial account statements and/or other personal records for any indications of actual or attempted identity theft or fraud.

88. Plaintiff Cimino recently learned of fraudulent activity on her bank account when her debit card was used to make a purchase that she did not authorize. The fraudulent transaction was done on the same payment card that Plaintiff used to purchase products on Defendant's website.

89. Plaintiff has had to spend valuable time dealing with this fraudulent use of her payment card and otherwise responding to and attempting to mitigate the impact the Data Breach has had on her life.

90. Plaintiff Cimino has suffered actual injury from having her PII compromised and misused as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Cimino; (b) violation of her privacy rights; (c) the theft of her PII; (d) loss of the benefit of the bargain, and (e) imminent and impending injury arising from the increased risk of identity theft and fraud.

///

91. Plaintiff Cimino provided her PII to Lazarus Naturals and/or its affiliates in conjunction with the products she obtained.

92. Plaintiff Cimino is now very concerned about future identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. The Data Breach has caused Plaintiff Cimino to suffer significant fear, anxiety, and stress, which has been compounded by the fact that her name, contact information, financial account numbers, and other intimate details are at the hands of criminals, and by the fact that her financial account was frozen because of a fraudulent transaction.

94. As a result of the Data Breach, Plaintiff Cimino anticipates spending considerably more time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Cimino will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come. In fact, Plaintiff Cimino has received an increased number of spam calls, texts and emails since the Data Breach.

95. Plaintiff Cimino has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches, especially in light of Defendant's recent history of multiple data breaches of its network and systems.

CLASS ALLEGATIONS

96. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated.

97. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the data breach announced by Defendant in or around August 2023, including all such individuals who were sent notice of the Data Breach (the "Nationwide Class").**

98. The Florida Subclass, which Plaintiff Cimino seeks to represent, comprises:

> **All persons residing in Florida whose PII was compromised in the data breach announced by Defendant in or around August 2023, including all such individuals who were sent notice of the Data Breach (the "Florida Subclass).**

99. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

100. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

101. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are roughly 42,000 individuals whose PII may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

102. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' PII for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

103. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

104. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

105. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

106. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

107. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

108. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

109. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

110. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the PII of Class Members, Defendant may continue to

refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

111. Further, Defendant have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

112. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

i. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CLAIMS FOR RELIEF

COUNT I

Negligence
(On Behalf of Plaintiff and the Nationwide Class)

113. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

114. As a condition of using Defendant's products and services, Plaintiff and Class Members, as current and former users, are obligated to provide Defendant and/or their affiliates with certain PII, including but not limited to, their name, address, email address, and payment card information, including credit/debit card number (in combination with security code, access code, password or PIN for the account), and other PII.

115. Plaintiff and Class Members entrusted their PII to Defendant and their affiliates on the premise and with the understanding that Defendant would safeguard their information, use

their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

116. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

117. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

118. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

119. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

120. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's business as an online retailer, for which the diligent protection of PII is a continuous forefront issue.

121. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

122. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant.

123. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

124. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

125. Defendant had and continues to have a duty to adequately and promptly disclose that Plaintiff's and Class Members' PII within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

126. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

127. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

128. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII during the time the PII was within its possession or control.

129. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

130. These foregoing frameworks are existing and applicable industry standards in the technology industry, and Defendant failed to comply with these accepted standards thereby opening the door to the threat actors, which resulted in the Data Breach.

131. Defendant improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

132. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect customer PII in the face of increased risk of theft.

133. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

134. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

135. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

136. There is a close causal connection between Defendant's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

137. Additionally, Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Lazarus Naturals' duty in this regard.

138. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

139. Defendant's violation of Section 5 of the FTCA constitutes negligence *per se.*

140. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

142. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's services they received.

143. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II

Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

144. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

145. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for providing products and services to current and former customers.

146. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiff and Class Members.

147. The money that users like Plaintiff paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

148. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

149. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

150. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that the borrowers paid for.

151. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III

Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide Class)

152. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

153. This count is pleaded in the alternative to Count II (Unjust Enrichment) above.

154. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

155. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit Plaintiff and the Class (all customers entering into the contracts), as Defendant's business is for services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

156. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

///

///

157. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized and malicious threat actors as part of the Data Breach.

158. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

159. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

160. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV

Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

161. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

162. This count is pleaded in the alternative to Counts II (Unjust Enrichment) and III (Breach of Express Contract) above.

163. Plaintiff's and Class Members' PII was provided to Defendant in exchange for the goods and the services that Defendant provided to Plaintiff and Class Members.

164. Plaintiff and Class Members agreed to pay Defendant for such goods and services.

165. Defendant and the Plaintiff and Class Members entered into these implied contracts which included an understanding that Defendant would provide adequate data security. This understanding was separate and apart from any express contracts concerning the security of

Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

166. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members was only used in accordance with the parties' contractual obligations.

167. Defendant was, therefore, required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

168. Under these implied contracts which included data security services and obligations, Defendant was further obligated to provide Plaintiff and all Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

169. However, Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII and timely detect the Data Breach, resulting in the harms now alleged herein.

170. Indeed, Defendant further breached these implied contracts by providing untimely notification to Plaintiff and Class Members who are already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

171. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

172. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of their bargain with Defendant.

///

///

173. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff nor Class Members, nor any reasonable person would have entered into such contracts with Defendant.

174. As a result of the Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

175. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

176. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V

Violation of Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. 501.201 through 501.213, *et seq.*
(On Behalf of the Florida Subclass)

177. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

178. Plaintiff Cimino, Florida Subclass Members, and Defendant are "persons" as defined by Fla. Stat. 501.201 through 501.213, *et seq.*

179. Defendant advertised, offered, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida, as Fla. Stat. 501.201 through 501.213, *et seq.*

180. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Fla. Stat. 501.201 through 501.213, *et seq.*, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is; and

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

181. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Cimino's and Florida Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiff Cimino's and Florida Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' PII;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Cimino's and Florida Subclass Members' PII, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cimino's and Florida Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Cimino's and Florida Subclass Members' PII; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cimino's and Florida Subclass Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

182. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' PII.

183. Defendant intended to mislead Plaintiff Cimino and Florida Subclass Members and induce them to rely on their own misrepresentations and omissions.

184. Defendant also failed to implement and maintain reasonable security measures to protect Plaintiff Cimino's and Florida Subclass Members' PII from unauthorized access, acquisition, destruction, use, modification, or disclosure, in violation of Fla. Stat. 501.201 through 501.213.

185. Defendant acted intentionally, knowingly, and maliciously to violate Fla. Stat. 501.201 through 501.213, and recklessly disregarded Plaintiff Cimino's and Florida Subclass Members' rights.

186. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Cimino and Florida Subclass Members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the Data Breach.

187. Plaintiff Cimino and the Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

///

///

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Florida Subclass, and appointing Plaintiff and their Counsel to represent the certified Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and

integrity of the personal identifiable information of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of its systems;

ix. requiring Defendant to conduct regular database scanning and securing checks;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifiable information, as well as protecting the personal identifiable information of Plaintiff and Class Members;

xi. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifiable information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifiable information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final

judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully submitted this the 14th day of August 2023.

s/ Paul B. Barton
Paul B. Barton, OSB No. 100502
Alex Graven, OSB No. 153443
OLSEN BARTON LLC
4035 Douglas Way, Suite 200
Lake Oswego, OR 97035
Tel: (503) 468-5573
E: paul@olsenbarton.com
E. alex@olsenbarton.com

Mason A. Barney (*pro hac vice to be filed*)
Tyler J. Bean (*pro hac vice to be filed*)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com

Attorneys for Plaintiff and the Putative Class